

Appl. No. 10/081,908  
Amendment and/or Response  
Reply to Office action of 10 March 2006

Page 2 of 14

**Amendments to the Claims:**

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

1. A method for evaluating ~~the random numbers generated by a random number generator~~, the method comprising ~~the steps of:~~
  - generating a stream of random numbers;
  - determining an average number of bits that have a value of a predetermined logic value at a ~~specific~~, predefined range of intervals;
  - ~~applying each of the average number of bits indicative of said predetermined logic value to~~ using an exponential averaging operation (A); and,
  - determining whether ~~said the random number generator is properly providing random numbers generated random numbers are unpredictable by comparing the an~~ output of ~~said the~~ exponential averaging operation (A) to a predetermined acceptance range.
2. The method of claim 1, wherein the value of ~~said the~~ predetermined logic value is one of 1's and 0's.
3. The method of claim 1, ~~further comprising the step of including~~ determining that ~~said the random number generator is not properly providing random numbers generated random numbers are predictable when the output of said the exponential averaging operation (A) falls outside said the predetermined acceptance range.~~

Appl. No. 10/081,908  
Amendment and/or Response  
Reply to Office action of 10 March 2006

Page 3 of 14

4. The method of claim 1, ~~further comprising the step of including~~ notifying that ~~said the random number generator is not properly providing random numbers generated random sequences are predictable~~ when the output of ~~said the~~ exponential averaging operations (A) falls outside ~~said the~~ predetermined acceptance range.

5. The method of claim 1, ~~further comprising the step of including~~ updating all ~~said the~~ exponential averaging operations (A) each time a new bit is generated.

6. The method of claim 5, wherein ~~said the~~ exponential averaging operation (A) is updated according to the following equation:

$$A_{\text{new}} = \alpha \cdot A_{\text{old}} + b,$$

wherein  $\alpha = 1 - 1/n$ ,  ~~$n > 1$~~ , and  $\alpha$  falls between 0 and 1 ( $0 < \alpha < 1$ ), and wherein  $b$  is a value ~~comprising of~~ 1 when the average number of bits ~~predetermined logic value~~ is obtained, otherwise 0.

7. The method of claim 1, ~~further comprising the step of including~~ generating a new set of random sequences when the output of ~~said the~~ exponential averaging operation falls outside ~~said the~~ predetermined acceptance range.

8. The method of claim 6, wherein ~~said the~~ predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where  $c$  is selected to achieve a desired security threshold level.

Appl. No. 10/081,908  
Amendment and/or Response  
Reply to Office action of 10 March 2006

Page 4 of 14

9. A method for evaluating ~~the random numbers generated by a random number generator~~, the method comprising ~~the steps of~~:

(a) generating a stream of random numbers of binary bits using ~~said the~~ random number generator;

(b) determining an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals;

~~—(c) computing using an exponential averaging operation (A) on the average number of bits indicative of said predetermined logic value;~~

(~~dc~~) comparing the ~~an~~ output of ~~said the~~ exponential averaging operation (A) to a predetermined acceptance range; and,

(~~ed~~) determining that ~~said the random number generator is not properly operating generated random numbers are predictable when the output of said the computed exponential averaging operation (A) falls outside said the predetermined acceptance range.~~

10. The method of claim 9, ~~further comprising the step of: including~~ repeating ~~said steps (a) - (ed) until said computed the output of the exponential averaging operation (A) repeatedly falls outside said the predetermined acceptance range more than a predefined number of times.~~

11. The method of claim 9, ~~further comprising the step of: including~~ notifying that ~~the random number generator is not properly operating non-random numbers are generated when said the output of the computed exponential averaging operation (A) repeatedly falls outside said the predetermined acceptance range more than a predefined number of times.~~

12. The method of claim 9, ~~further comprising the step of: including~~ generating a new set of random numbers when ~~said the output of the computed exponential averaging operation (A) repeatedly falls outside said the predetermined acceptance range more than a predefined number of times.~~

Appl. No. 10/081,908  
 Amendment and/or Response  
 Reply to Office action of 10 March 2006

Page 5 of 14

13. The method of claim 9, ~~further comprising the step of including~~ updating said ~~the~~ exponential averaging operation (A) according to the following equation:

$$A_{\text{new}} = \alpha \cdot A_{\text{old}} + b,$$

wherein  $\alpha = 1 - 1/n$ ,  ~~$n > 1$  and  $\alpha$  falls between 0 and 1 ( $0 < \alpha < 1$ )~~, and wherein  $b$  is a value ~~comprising of 1~~ when the average number of bits ~~predetermined logic value~~ is obtained, otherwise 0.

14. The method of claim 13, wherein ~~said the~~ predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where  $c$  is selected to achieve a desired security threshold level.

15. An apparatus ~~for evaluating the random numbers generated by a random number~~, comprising:

a random generator unit for generating ~~substantially random sequences of~~ binary bits;

a detector unit, coupled to ~~the an~~ output of ~~said the~~ random generator unit, for detecting whether ~~said the~~ generated random sequences are unpredictable; and,

a switching unit, coupled to the output of ~~the s~~ said random generator unit and ~~an output of the said~~ detector unit, for disabling the flow of ~~the said generated random sequences for a subsequent application~~ when ~~said the~~ generated random sequences are determined to be predictable,

wherein

the detector unit is configured to:

determine an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals ~~is determined and applied to using exponential averaging operations (A), and wherein,~~

determine that the sequence is predictable if the output of said the exponential averaging operations (A) falls outside a predetermined acceptance range, ~~determining that said generated random sequences are predictable.~~

Appl. No. 10/081,908  
Amendment and/or Response  
Reply to Office action of 10 March 2006

Page 6 of 14

16. The apparatus of claim 15, further comprising means for transmitting an alarm signal when the output of ~~said the~~ exponential averaging operation ~~(A)~~ falls outside ~~said the~~ predetermined acceptance range.

17. The apparatus of claim 15, wherein ~~said the~~ exponential averaging operation ~~(A)~~ is performed according to the following equation:

$$A_{\text{new}} = \alpha \cdot A_{\text{old}} + b,$$

wherein  $\alpha = 1 - 1/n$ ,  ~~$n > 1$  and  $\alpha$  falls between 0 and 1 ( $0 < \alpha < 1$ )~~, and wherein  $b$  is a value ~~comprising of 1 when the average number of bits predetermined~~ logic value is obtained, otherwise 0.

18. The apparatus of claim 17, wherein ~~said the~~ predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where  $c$  is selected to achieve a desired security threshold level.

19. A machine-readable medium having stored thereon data representing sequences of instructions, and the sequences of instructions which, when executed by a processor, cause the processor to:

generate a stream of random bits;

determine an average number of bits that have a value of a predetermined

logic value at a specific, predefined range of intervals;

~~perform using an~~ exponential averaging operation ~~(A)~~ on the number of bits indicative of ~~said the~~ predetermined logic value; and,

compare ~~the an~~ output of ~~said the~~ exponential averaging operations ~~(A)~~ to a predetermined acceptance range.

Appl. No. 10/081,908  
Amendment and/or Response  
Reply to Office action of 10 March 2006

Page 7 of 14

20. The machine-readable medium of claim 19, wherein said the generated random numbers are determined to be predictable when said the computed exponential averaging operation-(A) falls outside said the predetermined acceptance range.

21. The machine-readable medium of claim 19, wherein said the exponential averaging operation-(A) is performed according to the following equation:

$$A_{\text{new}} = \alpha \cdot A_{\text{old}} + b,$$

wherein  $\alpha = 1 - 1/n$ ,  ~~$n > 1$  and  $\alpha$  falls between 0 and 1 ( $0 < \alpha < 1$ )~~, and wherein  $b$  is a value ~~comprising of 1~~ when the average number of bits predetermined logic value is obtained, otherwise 0.

22. The machine-readable medium of claim 21, wherein said the predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where  $c$  is selected to achieve a desired security threshold level.